REMARKS/ARGUMENTS

Claims 1-8 now stand n the present application, claims 1, 4 and 5 having been amended, and claims 9-10 and 16-20 having been canceled. Reconsideration and favorable action is respectfully requested in view of the above amendments and the following remarks.

In the Office Action, the Examiner has objected to the specification as introducing new matter. While Applicants do not agree with the Examiner's statement that new matter was added to the application by the amendment dated May 2, 2008, in that the amended material would be readily recognized by those skilled in the art from reading the present application and in that the Examiner's statement as to how URLs are typically constituted does not establish that the amended material is new matter. In any event, in order to further the prosecution of this case, Applicants have canceled the material objected to by the Examiner. Accordingly, the Examiner's objection to the specification is believed to have been overcome.

The Examiner has rejected claims 16-20 under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. As noted above, Applicants have canceled claims 16-20 and, therefore, the Examiner's rejection of these claims is moot.

The Examiner has rejected claim 5 under 35 U.S.C. § 101 as not falling within one of the four statutory categories of invention. The Examiner's rejection in this regard is not understood since it is clear that claim 5 is directed to a method of operating a server computer and the retrieving limitations in the claim clearly are not capable of

being performed mentally, verbally or without being tied to a machine as alleged by the Examiner. In order to further the prosecution of this case, however, Applicants have amended claim 5 in order to emphasize that the methodology is performed by at least one processor of a server computer. Accordingly, the Examiner's § 101 rejection of claim 5 is believed to have been overcome.

The Examiner has rejected claims 1-10 and 16-20 under 35 U.S.C. § 102(e) as being anticipated by Bisbee et al. ("Bisbee"). Applicants respectfully traverse the Examiner's § 102 rejection.

Applicants have amended independent claims 1, 4 and 5 to make it clear that the present invention involves the checking of a file's digital signature being carried out by the server computer in response to a request from another computer for the file. Independent claim 7 already clearly required this feature.

Bisbee, similarly to all the other prior-art cited in the long history of this case, leaves the other computer (the one requesting the file) to check a digital signature applied to the file. In Bisbee, the signature which is checked by the requesting computer represents a certification by the trusted repository storing the file. That certification provides evidence that the file is authentic and has not been altered since the file's originator signed the file.

This can be seen from, for example, Bisbee at column 13, line 67 to column 14, lines 7-8, where the document signed by the two parties – denoted $S_c(S_a(\text{Object}))$ – is further signed by the Trusted Repository to create $S'_{TR}(S_c(S_a(\text{Object})))$ which is transmitted to both S_b and S_c. Given that the signed document is sent, it is clear that

checking of the Trusted Repository's signature is to be carried out by the receiver (i.e., S_b or S_c in this instance).

The sentence cited by the Examiner at column 15, lines 12 -13 of Bisbee states that the Trusted Repository (in this particular part of Bisbee called a Trusted Custodial Utility – see column 14, lines 65-67) prints and issues certified documents. This is expanded upon in column 15, lines 44-53 which indicates that the printed certified document should have some form of 'indicum or legend' that certifies the document (presumably as corresponding to the original and being authentically signed). The Bisbee specification when read in its entirety suggests that this is a paper-based equivalent of the electronic signature Bisbee applies to electronic documents before transmitting them to third parties. See, for example, Bisbee at column 10, lines 34-38.

Thus, it should be clear that Bisbee is teaching that the Trusted Repository's digital signature (the electronic form of 'certification') is to be checked by the recipient of the certified document – in exactly the same way a recipient of the certified paper document would be expected to check the 'watermark, hologram or similar' which constitutes the 'indicum or legend' denoting the Trusted Repository's certification of the paper document. To this extent, Bisbee is similar to the Microsoft Authenticode software discussed in the last paragraph of page 5 of the present application. It follows that Bisbee suffers the same problems as the Authenticode software discussed in the first paragraph of page 6 of the present application. If, for example, a malicious hacker were able to maliciously edit an electronic version of a commercial agreement between two respected individuals so that it appeared to be a commercial agreement between a

respected individual and a known crook, then the altered document might still be accessible to others. They might have digital signature technology on their computers which would indicate that the agreement had been altered, but they would not necessarily choose to use it.

The other important passages cited by the Examiner should be read in this context. For example, Bisbee at column 3, lines 9-16 teaches that the originator of a document digitally signs that document and sends it to the trusted repository together with a certificate in which a Certification Authority certifies that the signature really is that of the originator. The trusted repository then checks that the digital signature is that of the originator and that the document has been unaltered since the originator signed it. The trusted repository then certifies that document by:

i) adding date and time stamps, and a certificate which enables those checking the trusted repository's signature to check that the Certification Authority certifies that the signature really is that of the trusted repository; and

ii) signing the combination of the date and time stamps, certificate and the original document signed by the originator.

Thus, the digital signature of the trusted repository serves the function of certifying the integrity of the document and signature of the originator.

Bisbee at column 7, lines 22-33 teaches that the Document Authentication System (DAS) can verify that the document it receives is exactly that which was executed and transmitted by the originator. That integrity check is recorded by having the DAS date and time stamp the document and then sign the combination. This

second digital signature is the 'certification' of the document. Similarly, Bisbee at column 11, lines 27-41 teaches that the 'certification' of the signed document by the trusted repository is carried out when the original document is received by the trusted repository.

In short, Bisbee teaches that documents it receives are checked for integrity and authenticity and then certified. That certification is evidenced by applying date and time stamps and a digital signature to the document. The trusted repository may then later send the certified document to a recipient – i.e., the trusted repository will send the document signed with its own digital signature. It is up to the recipient to check that digital signature if they wish to check the authenticity and integrity of the document.

In contrast, Applicants' invention involves the integrity of a document being checked by the server computer in response to a request for that document. The server computer may, or may not, then provide evidence that the check has been carried out in the form of a digital signature. In Applicants' described embodiment, no digital signature is applied by the server computer to the document. See present application at Fig. 4, item 408. This overcomes the problems discussed in the first paragraph of page 6 of the present application. Maliciously altered documents are simply not sent to those that request the document. This provides a more secure solution to the problem of the serving of maliciously altered documents than Bisbee, for the reasons explained above.

For all of the above reasons, it is respectfully submitted that independent claims 1, 4, 5, and 7 patentably define over Bisbee. The dependent claims are also patentable at least by virtue of their dependency from one of the independent claims.

Therefore, in view of the above amendments and remarks, it is respectfully requested that the application be reconsidered and that all of claims 1-8, now standing in the application, be allowed and that the case be passed to issue. If there are any other issues remaining which the Examiner believes could be resolved through either a supplemental response or an Examiner's amendment, the Examiner is respectfully requested to contact the undersigned at the local telephone exchange indicated below.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
Chris Comuntzis
Reg. No. 31,097

CC:lmr
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100